

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)

1033-T00534C

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature_____

Typed or printed Jason D. Smith
name _____

Application Number

10/605,689

Filed

2003-10-17

First Named Inventor

James M. Doherty

Art Unit

2137

Examiner

GERGISO, Techane

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

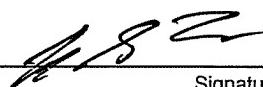
This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).

Note: No more than five (5) pages may be provided.

I am the

applicant/inventor.



Signature

assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

Jeffrey G. Toler

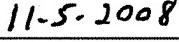
attorney or agent of record.
Registration number _____.

Typed or printed name

512-327-5515

Telephone number

attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 38,342


Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

*Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: James M. Doherty, et al.

Title: INTRUSION DETECTION

App. No.: 10/605,689 Filed: October 17, 2003

Examiner: GERGISO, Techane Group Art Unit: 2137

Customer No.: 60533 Confirmation No.: 2688

Atty. Dkt. No.: 1033-T00534C

MS: AF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**REMARKS IN SUPPORT OF PRE-APPEAL BRIEF
REQUEST FOR REVIEW**

Dear Sir:

In response to the Final Office Action mailed August 6, 2008, and further pursuant to the Notice of Appeal and Pre-Appeal Brief Request for Review submitted herewith, Applicants respectfully request review and reconsideration of the Final Office Action in view of the following issues.

Claims 1-2, 4-16 and 18-25 are Allowable

The Office has rejected claims 1-2, 4-16 and 18-25, under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 6,647,400 (“Moran”), in view of U.S. Application No. 2002/0129264 (“Rowland”).

The cited portions of Moran and Rowland, individually or in combination, do not disclose or suggest the specific combination of claim 1. For example, the cited portions of Moran and Rowland fail to disclose or suggest that upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database where the entry identifies a possible intrusion in a host, and issuing a command to an operating system of the host to bring the host to a single user state, as in claim 1.

The Office admits that Moran fails to teach this feature. *Office Action at page 3.* The Office then takes the position that Rowland teaches this feature at paragraphs 0037, 0053, 0065, 0145 and 0148. Rowland, at paragraph 0037, notes that a log handler 203 logs system events locally or remotely. Paragraph 0053 of Rowland discloses the logging handler can accept a variety of formats and notification can be sent in a number of ways but fails to disclose or suggest bringing a host to a single user state.

Paragraph 0065 describes functionality of an action handler 204 and describes that the action handler 204 can block hosts, users, networks, running commands, logging events, disabling interfaces, disabling a computer, sending email, paging personnel and providing on-screen alerts. However, paragraph 0065 fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state.

Paragraph 0145 also fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state. Paragraph 0145 of Rowland discusses that an intrusion control agent 1302 performs certain functions at a host computer system including disabling of the network interfaces, shutdown of active user accounts, locating and logging suspicious activities, notifying a central controller of its actions, requesting collection of forensic evidence, moving between other affected client systems and attempting to contain the intrusion situation. Paragraph 0145 of Rowland mentions shutting down active user account. However, shutting down active user accounts is distinct from bringing the host to a single user state. In fact, Rowland appears to be suggesting bringing the host to a zero user state by shutting down the active user accounts. Thus, none of these recited functions disclose or suggest issuing a command to an operating system of the host to bring the host to a single user state, as in claim 1.

Paragraph 0148 similarly fails to disclose or suggest issuing a command to an operating system of the host to bring the host to a single user state, as in claim 1. Rather, paragraph 0148 of Roland describes a known intrusion agent 1305 which is designed to specifically look for an alarm on signs of known intrusion. However, nothing in paragraph 0148 discloses or suggests bringing the host to a single user state.

Therefore, the cited portions of Moran and Rowland, individually or in combination, fail to disclose or suggest the specific combination of claim 1. Hence, claim 1 is allowable. Claims 2 and 4-9 are allowable, at least by virtue of their dependence from an allowable claim. Further,

claims 2 and 4-9 recite additional features not disclosed or suggested by the cited portions of Moran and Rowland.

For example, the cited portions of Moran and Rowland, individually or in combination, do not disclose or suggest that a first remote database and a second remote database are located on a single server or a plurality of servers belonging to a local area network, as in claim 4. The Office takes the position that this feature is disclosed by Rowland at paragraph 0037, 0053 and 0147. Paragraphs 0037 and 0053 of Rowland were discussed above and fail to disclose or suggest that a first remote database and a second remote database are located on a single server or a plurality of servers belonging to a local area network. Rather, the cited paragraphs indicate that the logging may be done on a remote server but does not disclose or suggest that the first remote database and the second remote database are located on a single server or on a plurality of servers belonging to a local area network. Paragraph 0147 of Rowland discusses a host scanning agent 1304 designed to perform a host vulnerability assessment and vulnerability detection from within the host but fails to disclose or suggest the first remote database and the second remote database are located on a single server or a plurality of servers belonging to a local area network.

The cited portions of Moran and Rowland, individually or in combination, do not disclose or suggest the specific combination of claims 10, 15 and 18. For example, the cited portions of Moran and Rowland fail to disclose or suggest a command being issued to an operating system of a host to bring the host to a single user state, as in claim 10, computer readable program code comprising executable instructions to issue a command to an operating system of a host to bring the host to a single user state, as in claim 15 and issuing a command to an operating system of a host to bring the host to a single user state, as in claim 18.

The Office admits that Moran fails to teach this feature. *Office Action at page 3*. The Office then takes the position that Rowland teaches this feature at paragraphs 0037, 0053, 0065, 0145 and 0148. Rowland, at paragraph 0037, simply notes that a log handler 203 logs system events locally or remotely. Paragraph 0053 of Rowland discloses the logging handler can accept a variety of formats and notification can be sent in a number of ways. Both paragraphs fail to disclose or suggest bringing a host to a single user state.

Paragraph 0065 describes functionality of an action handler 204 and describes that the action handler 204 can issue various commands. However, paragraph 0065 fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state.

Paragraph 0145 also fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state. Paragraph 0145 of Rowland discusses that an intrusion control agent 1302 performs certain functions at a host computer system including shutting down of active user accounts. However, shutting down active user accounts is distinct from bringing the host to a single user state. In fact, Rowland appears to be suggesting bringing the host to a zero user state by shutting down the active user accounts. Thus, none of these recited functions disclose or suggest a command being issued to an operating system of a host to bring the host to a single user state, as in claim 10, computer readable program code comprising executable instructions to issue a command to an operating system of a host to bring the host to a single user state, as in claim 15 and issuing a command to an operating system of a host to bring the host to a single user state, as in claim 18.

Paragraph 0148 of Roland describes a known intrusion agent 1305 which is designed to specifically look for an alarm on signs of known intrusion. However, nothing in paragraph 0148 discloses or suggests bringing the host to a single user state.

Therefore, the cited portions of Moran and Rowland, individually or in combination, fail to disclose or suggest the specific combination of claims 10, 15 and 18. Hence, claims 10, 15 and 18 are allowable.

Claims 11-14 are allowable, at least by virtue of their dependence from allowable claim 10. Claim 16 is allowable, at least by virtue of its dependence from allowable claim 15. Claims 19-25 are allowable, at least by virtue of their dependence from allowable claim 18.

CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested, or rendered obvious by the cited portions of the references applied in the Final Office Action. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the objections and rejections, as well as an indication of the allowability of each of the pending claims. The Examiner is invited to contact the undersigned attorney at the telephone number listed below if such a call would in any way facilitate allowance of this application.

The Commissioner is hereby authorized to charge any fees, which may be required, to credit any overpayment, to Deposit Account Number 50-2469.

Respectfully submitted,

11-5-2008

Date


Jeffrey G. Toler, Reg. No. 38,342

Attorney for Applicants

Toler Law Group, Intellectual Properties
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)